JAY EDELSON*
(jedelson@edelson.com)
RAFEY S. BALABANIAN*
(rbalabanian@edelson.com)
ARI J. SCHARG*
(ascharg@edelson.com)
CHRISTOPHER L. DORE*
(cdore@edelson.com)
EDELSON MCGUIRE LLC
350 North LaSalle Street, Suite 1300
Chicago, Illinois 60654
Tel: (312) 589-6370
**Admitted Pro Hac Vice*

LAURENCE D. KING (SBN 206423)
(lking@kaplanfox.com)
LINDA M. FONG (SBN 124232)
(lfong@kaplanfox.com)
KAPLAN FOX &KILSHEIMER LLP
350 Sansome Street, Suite 400
San Francisco, CA 94104
Tel: (415) 772-4700

ATTORNEYS FOR PLAINTIFFS AND THE PUTATIVE CLASSES

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

IN RE LINKEDIN USER PRIVACY LITIGATION	) Case No.12-cv-03088-EJD)) **CONSOLIDATED CLASS ACTION COMPLAINT FOR:**)) **(1) Violations of Cal. Bus. & Prof. Code § 17200;**) **(2) Violations of Cal. Civ.Code § 1750;**) **(3) Breach of Contract;**) **(4) Breach of the Implied Covenant of Good Faith and Fair Dealing;**) **(5) Breach of Implied Contracts;**) **(6) Negligence;**) **(7) Negligence Per Se.**)) **DEMAND FOR JURY TRIAL**

Plaintiffs Katie Szpyrka and Scott Shepherd, by and through their attorneys, upon personal knowledge as to themselves and their own acts and experiences, and upon information and belief as to all other matters, alleges as follows:

NATURE OF THE ACTION

1. Plaintiffs Katie Szpyrka and Scott Shepherd bring this consolidated class action complaint against LinkedIn Corporation ("LinkedIn") for failing to properly safeguard its users' digitally stored personally identifiable information ("PII"), including e-mail addresses, passwords, and login credentials. LinkedIn violated its own User Agreement and Privacy Policy by failing to utilize long-standing industry standard protocols and technology to protect Plaintiffs and the Classes' PII.

2. LinkedIn is an Internet company that owns and operates the website www.LinkedIn.com—a social networking website with over 120 million registered users worldwide.

3. Through its Privacy Policy, LinkedIn promises its users that "[a]ll information that [they] provide [to LinkedIn] will be protected with industry standard protocols and technology."[1] In direct contradiction to this promise, however, LinkedIn failed to comply with basic industry standards by maintaining millions of users' PII in its servers' databases in a weak encryption format, and without implementing other crucial security measures.

4. Sometime this year, hackers infiltrated LinkedIn's servers and accessed database(s) containing its users' PII. After retrieving this data, the hackers publicly posted over 6 million LinkedIn users' passwords online. Because LinkedIn used insufficient encryption methods to secure the user data, hackers were able to easily decipher a large number of the passwords.

[1] LinkedIn "Privacy Policy," http://www.linkedin.com/static?key=privacy_policy&trk=hb_ft_priv (last visited September 19, 2012).

5. While some security threats are unavoidable in a rapidly developing technological environment, LinkedIn's failure to comply with long standing industry standard encryption protocols jeopardized its users' PII, and diminished the value of the services provided by Defendant—as guaranteed by its own contractual terms.

PARTIES

6. Plaintiff Katie Szpyrka is a natural person and resident of the State of Illinois. Plaintiff Szpyrka is a registered user of LinkedIn's services.

7. Plaintiff Scott Shepherd is a natural person and resident of the State of California. Plaintiff Shepherd is a registered user of LinkedIn's services.

8. Defendant LinkedIn Corporation is a corporation incorporated and existing under the laws of the State of Delaware, with its principal place of business located at 2029 Stierlin Court, Mountain View, California 94043. LinkedIn does business throughout the State of California and the United States.

JURISDICTION AND VENUE

9. This Court has original jurisdiction over this action pursuant to 28 U.S.C. § 1331. The Court also has subject matter jurisdiction pursuant to § 1332(d), because (a) at least one member of the putative class is a citizen of a state different from Defendant, (b) the amount in controversy exceeds $5,000,000.00, exclusive of interest and costs, and (c) none of the exceptions under the subsection apply to this action.

10. Venue is proper in this District under 28 U.S.C. § 1391(a) because Defendant maintains its headquarters and principal place of business in this District and a substantial part of the events giving rise to Plaintiffs' Complaint occurred in this District.

FACTUAL BACKGROUND

11. LinkedIn's website states that it "operates the world's largest professional network on the Internet with more than 120 million members in over 200 countries and territories [and] represents a valuable demographic for marketers with an affluent & influential

membership."[2]

12. A customer may sign up for a membership at www.LinkedIn.com by providing a valid e-mail address and a registration password. LinkedIn then stores these credentials in databases located on its servers. Once registered, users build personal "profiles" by providing LinkedIn with various types of demographic, occupational, and cultural information, including employment and educational history.

13. Defendant also offers users the ability to upgrade to a paid "premium" account, with prices ranging from $19.95 to $99.95 per month.

14. Regardless of whether a user signs up for a free or premium account, LinkedIn asserts through its Privacy Policy that it will safeguard its users' sensitive PII, specifically that: "All information that you provide will be protected with industry standard protocols and technology." Plaintiffs and the Classes agreed to LinkedIn's User Agreement and Privacy Policy in order to register and use LinkedIn's services.

15. Importantly, Plaintiffs and the members of the Classes relied on LinkedIn's representation that it uses "industry standard protocols and technology" to preserve the integrity and security of their personal information in agreeing to create an account and provide their PII to the company, and when deciding to purchase "premium" accounts.

LinkedIn Fails to Properly Encrypt its Users' PII

16. As introduced above, LinkedIn digitally stores millions of users' PII in a large-scale commercial database on its servers, and promises through its Privacy Policy that it uses "industry standard protocols and technology" to protect such PII.

17. However, and despite its contractual obligation to use best practices in storing user data, LinkedIn failed to utilize basic industry standard encryption methods. In particular, LinkedIn failed to adequately protect user data because it stored passwords in unsalted SHA1

[2] LinkedIn "About Us," http://press.linkedin.com/about (last visited September 19, 2012).

hashed[3] format. The problem with this practice is two-fold. First, SHA-1 is an outdated hashing function, first published by the National Security Agency in 1995. Secondly, storing users' passwords in hashed format without first "salting" the password runs afoul of conventional data protection methods, and poses significant risks to the integrity of users' sensitive data.

18. Industry standards require at least the additional process of adding "salt" to a password before running it through a hashing function—a process whereby random values are combined with a password before the text is input into a hashing function. This procedure drastically increases the difficulty of deciphering the resulting encrypted password.

19. The more common standard practice is to salt passwords before inputted into a hash function, to then salt the resulting hash value, and again run the hash value through a hashing function. Finally, that fully encrypted password is stored on a separate and secure server apart from all other user information. Defendant's data protection procedures fall well short of this level of security.

20. LinkedIn failed to use a modern hashing and salting function, and therefore drastically exacerbated the consequences of a hacker bypassing its outer layer of security. In so doing, Defendant violated its Privacy Policy's promise to comply with industry standard protocols and technology for data security.

The Attack on LinkedIn's Database

21. Preliminary reports indicate that LinkedIn's servers were breached through a common hacking method known as an "SQL injection" attack. This hacking technique involves exploiting weaknesses existing in a company's website to penetrate deeper into back-end servers that contain databases of sensitive user information.

22. A failure by LinkedIn to adequately protect its website against SQL injection attacks—in conjunction with improperly securing its users' PII—would demonstrate that the

[3] In simplest terms for purposes of this Complaint, "hashing" refers to the process by which a password is inputted into a cryptographic hash function and converted into an unreadable, encrypted format.

company employed a troubling lack of industry standard security measures and protocols.

23. In fact, the Federal Trade Commission ("FTC") has filed complaints against corporations claiming to secure customer data while remaining vulnerable to SQL injection attacks.[4] In the referenced case, the FTC filed a complaint in 2003 against the "Guess?" clothing company. The complaint alleges that despite a posted policy ensuring reasonable Internet security measures, "Guess?" stored customers' PII in an unencrypted database concomitantly with poor website security. The FTC argued that these practices constituted unfair or deceptive practices affecting commerce in violation of federal law.

24. Moreover, the National Institute of Standards and Technology ("NIST") provides basic network security checklists that enumerate steps to avoid SQL injection vulnerabilities.[5] The failure of a large company tasked with protecting millions of users' PII, such as LinkedIn, to act pursuant to these basic security checklists would further belie its assertion that it employed industry standard protocols and technology to secure its customers' PII.

25. Had LinkedIn used proper encryption methods, and a hacker were able to penetrate LinkedIn's network, he would be limited in his ability to inflict harm. For example, though a hacker still might be able to cause temporary internal havoc in the operation of the website, or "vandalize" the appearance of pages by altering its code, he would not be able to access user databases. Moreover, if LinkedIn used appropriate encryption methods—but still failed to secure its database—the stolen PII would be useless, as it would be indecipherable.

26. On June 6, 2012, a list of approximately 6.5 million hashed passwords retrieved from LinkedIn's database was publicly posted online by hackers. Because the passwords were only hashed with a weak hashing function (and not salted), individuals were able to quickly decipher a large contingency of the posted passwords in a matter of hours. It quickly became

---

[4] *In the Matter of Guess?, Inc. and Guess.com Inc.*, (Case No. C-4091) (FTC, July 30, 2003) (available at http://www.ftc.gov/os/2003/08/guesscomp.pdf).

[5] National Checklist Program Repository, http://checklists.nist.gov (last visited September 19, 2012).

apparent that the passwords belonged to LinkedIn users.

27. Only after third party observers publicly announced the origin of the password list did LinkedIn become aware that its security had even been breached and that confidential information had been removed. Initially, LinkedIn publicly responded by stating, "[o]ur security team continues to investigate this morning's reports of stolen passwords. At this time, we're still unable to confirm that any security breach has occurred."[6]

28. However, on June 9, 2012, LinkedIn admitted that it was not handling user data in accordance with best practices. LinkedIn stated that "one of our major initiatives was the transition from a password database system that hashed passwords, *i.e*. provided one layer of encoding, to a system that both hashed and salted the passwords, *i.e*. provided an extra layer of protection that is a widely recognized best practice within the industry. That transition was completed prior to news of the password theft breaking on Wednesday. We continue to execute on our security roadmap, and we'll be releasing additional enhancements to better protect our members."[7] But these actions were too little too late—LinkedIn's transition to industry standard data protection practices clearly occurred *after* its servers were breached, as the passwords publicly posted were, by its own admission, only hashed.

29. That LinkedIn did not recognize its databases had been compromised until it was informed through public channels provides further evidence that the company didn't adhere to industry standards. Specifically, LinkedIn did not implement, or it poorly implemented, an intrusion detection system to properly identify and quickly respond to attacks on its servers.

LinkedIn's Business Model

30. LinkedIn offers products and services in the form of online applications to be

[6] Updating Your Password on LinkedIn and Other Account Security Best Practices, http://blog.linkedin.com/2012/06/06/updating-your-password-on-linkedin-and-other-account-security-best-practices/ (last visited September 19, 2012).

[7] An Update On Taking Steps To Protect Our Members, http://blog.linkedin.com/2012/06/09/an-update-on-taking-steps-to-protect-our-members/ (last visited September 19, 2012).

used in conjunction with online social networks.

31. LinkedIn's consumers pay for LinkedIn's products and services both with actual dollars and with their PII. Put another way, in addition to a more conventional subscription fee, "free" account users buy products and services by paying LinkedIn in the form of contact information (first name, last name, and an email address). Put yet another way, LinkedIn users provide something valuable—access to their personal information—in exchange for LinkedIn's products and services, which include LinkedIn's promise to employ industry standard protocols and technology to safeguard their PII.

32. Even for customers that it does not directly charge using traditional legal tender, LinkedIn is able to generate earnings from users through the receipt of their PII. LinkedIn describes itself as a "unique social application-based advertising network." In other words, LinkedIn makes money by selling targeted advertising space, similar to a newspaper or television program.

33. But unlike traditional newspaper or television marketing, LinkedIn is a particularly attractive advertising platform because it possesses detailed demographic information that may be used to direct highly targeted ads to its customers.

34. If not for the inherent and quantifiable value of access to its users' PII, LinkedIn could not sustain financial viability, as a considerable portion of its user base are not "premium" members, and thus do not pay monthly fees. Thus, the promises contained in its Privacy Policy concerning the safeguarding of consumer data that LinkedIn receives in exchange for its products and services are vital to its business and to its consumers.

FACTS RELATING TO PLAINTIFFS

35. During the relevant time period, Plaintiff Katie Szpyrka was a registered account holder with LinkedIn. She registered with LinkedIn in or around late 2010.

36. Beyond simply being a registered user of LinkedIn, Plaintiff Szpyrka additionally paid a monthly fee to use LinkedIn's upgraded, premium services. From approximately late 2010

to November 2011, she paid $24.95 per month, and from December 2011 to the present she has paid $26.95 per month.

37. In signing up to utilize LinkedIn, Plaintiff Szpyrka submitted her first name, last name, e-mail address, and a unique password to LinkedIn.

38. In creating an account with Defendant, Plaintiff Szpyrka agreed to and relied upon LinkedIn's User Agreement and Privacy Policy, including the material term that "Personal information you provide will be secured in accordance with industry standard protocols and technology."

39. The monthly fees, or a portion thereof, that Szpyrka paid to LinkedIn was used by LinkedIn to pay for the administrative costs of data management and security, and to otherwise comply with its promise to use "industry standard protocols and technology" to protect the Premium Services Class members' PII.

40. Had Plaintiff Szpyrka known of Defendant's substandard security procedures and methods of protecting and storing her PII, she would have paid less, or not paid at all, for Defendant's services. Plaintiff Szpyrka did not receive the benefit of the bargain in that the services provided were worth less than she paid for them, and that she paid more than she otherwise would have based upon Defendant's User Agreement and Privacy Policy.

41. During the relevant time period, Plaintiff Shepherd was a registered account holder with LinkedIn. He registered with LinkedIn in or around May 2007. In signing up to utilize LinkedIn, Plaintiff Shepherd submitted his first name, last name, e-mail address, and a unique password to LinkedIn.

42. In creating an account with Defendant, Plaintiff Shepherd agreed to LinkedIn's User Agreement and Privacy Policy, including the material term that "Personal information you provide will be secured in accordance with industry standard protocols and technology."

43. On or about June 7, 2012, Plaintiff Shepherd received an email from LinkedIn informing him that his LinkedIn account and password were compromised, and he was provided

with instructions on how to reset his password. As a result of Defendant's action, and Plaintiff Shepherd's reliance on promises made by Defendant in its Privacy Policy to protect his PII, Plaintiff Shepherd had his PII compromised, exposing him to a heightened risk of identity theft, causing him distress related to his unsecured personal data, as well as distress related to the security of his other personal accounts being exposed and accessed without authorization.

44. Had Plaintiff Shepherd known of Defendant's substandard security procedures and methods of protecting and storing his PII, he would not have provided his personal and confidential information in exchange for access to Defendant's services. Plaintiff Shepherd did not receive the benefit of the bargain in that the services provided were not commensurate with the value of the personal information he provided in exchange, and Plaintiff provided more information than he otherwise would have based upon Defendant's User Agreement and Privacy Policy.

CLASS ALLEGATIONS

45. Plaintiffs Shepherd and Szpyrka, respectively, bring this action pursuant to Fed. R. Civ. P. 23(b)(2) and (3) on behalf of themselves and two Classes of similarly situated individuals, defined as

> **Data Breach Class:** All individuals and entities in the United States who had a LinkedIn account and whose personal information was compromised as a result of the data breach that occurred on or around June 6, 2012.
>
> **Premium Services Class:** All LinkedIn User Class Members who paid a monthly fee to LinkedIn for a premium account.

Excluded from the Classes are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and their current or former employees, officers and directors; (3) counsel for Plaintiffs and Defendant; (4) persons who properly execute and file a timely request for exclusion from the class; (5) the legal representatives, successors or assigns of any such excluded persons; (6) all

persons who have previously had claims similar to those alleged herein finally adjudicated or who have released their claims against Defendant; and (7) any individual who contributed to the unauthorized access of LinkedIn's database.

46. The exact number of the members of the Classes is unknown to Plaintiffs at this time, but on information and belief, there are approximately 6 million members in the Data Breach Class and hundreds of thousands of persons in the Premium Services Class, making joinder of each individual member impracticable. Ultimately, members of both Classes will be easily identified through Defendant's records.

47. Plaintiffs' claims are typical of the claims of all the other members of the Classes.

48. Plaintiffs will fairly and adequately represent and protect the interests of the other members of the Classes. Plaintiffs have retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Classes, and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Classes.

49. Absent a class action, most members of the Classes would find the cost of litigating their claims to be prohibitive and will have no effective remedy. The class treatment of common questions of law and fact is also superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants, and promotes consistency and efficiency of adjudication.

50. LinkedIn has acted and failed to act on grounds generally applicable to Plaintiffs and the other members of the Classes, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Classes.

51. The factual and legal bases of LinkedIn's liability to Plaintiffs and to the other members of the Classes are the same and resulted in injury to Plaintiffs and all of the other members of the Classes. Plaintiffs and the other members of the Classes have all suffered harm

as a result of LinkedIn's wrongful conduct.

52. There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Classes, and those questions predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include but are not limited to the following:

(a) whether LinkedIn failed to protect users' PII with industry standard protocols and technology;

(b) whether storing user e-mails and passwords in a partially unencrypted format complied with industry standard protocols and technology;

(c) whether LinkedIn's conduct described herein violated the Unfair Competition Law (Cal. Bus. & Prof. Code §§ 17200, *et seq*.);

(d) whether LinkedIn's conduct described herein violated the California Legal Remedies Act (Cal. Civ. Code §§ 1750, *et seq*.);

(e) whether LinkedIn's conduct described herein constitutes a breach of contract;

(f) whether LinkedIn's conduct described herein constitutes breach of the implied covenants of good faith and fair dealing;

(g) whether LinkedIn's conduct described herein constitutes breach of implied contracts;

(h) whether LinkedIn's conduct described herein was negligent and/or grossly negligent; and,

(i) whether LinkedIn's conduct constitutes negligence *per se.*

53. Plaintiffs reserve the right to revise the definitions of the Classes based on further investigation, including facts learned in discovery.

FIRST CAUSE OF ACTION
Violation of California's Unfair Competition Law
Cal. Bus.&Prof. Code §§ 17200, *et seq*.
(On Behalf of Plaintiffs and both Classes)

54. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

55. California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200, *et seq*., protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

56. The UCL prohibits any unlawful, unfair, or fraudulent business act or practice. A business practice need only meet one of the three criteria to be considered unfair competition. An unlawful business practice is anything that can properly be called a business practice and that at the same time is forbidden by law.

57. As described herein, Defendant's knowing and willful failure to safeguard and secure its users' sensitive PII violates the UCL.

58. Commonly accepted and widely practiced industry standards provide that sensitive PII stored in a commercial database should be not be accessible to extraction and simple decryption, and commercially reasonable methods to prevent such access are widely known throughout the security industry.

59. LinkedIn willfully and knowingly failed to expend the resources necessary to protect the sensitive data entrusted to it by Plaintiffs and the Classes in clear contradiction of accepted industry standards for database security and its own agreements. In creating the perception that it followed industry standard protocols for database protection, and explicitly stating as much, LinkedIn gained an unfair advantage over its competitors.

60. Additionally, LinkedIn was likely to deceive consumers by providing in its Privacy Policy that its users' PII would be "protected with industry standard protocols and technology."

61. By failing to maintain its users' PII in a properly encrypted database, LinkedIn failed to use commercially reasonable safeguards to protect its users' PII. Storing sensitive PII in

simple hashed values is not commercially reasonable and does not comport with industry standard protocols and technology, as promised.

62. By failing to employ industry standard protocols and technology to safeguard its users' personal data, LinkedIn violated its own written Privacy Policy and acted deceptively.

63. Defendant has violated the "unlawful" prong of the UCL because its conduct as alleged herein violated the Consumer Legal Remedies Act, Cal. Civ. Code §§ 1750 *et seq*.

64. LinkedIn's representations regarding its security procedures were likely to deceive the public because they were authoritative descriptions made in the contracts between LinkedIn and its users. Because PII privacy and security is likely to, and does, affect consumers' willingness to use and pay for a service, LinkedIn's representations were material.

65. Defendant has violated the unfair prong of the UCL because it operated a business that induced consumers to submit PII with the written assurance that the data would be protected through industry standard protocols and technology. However, Defendant knowingly failed to employ industry standard protocols and technology for data protection, causing the widespread exposure of its users' PII. Defendant engaged in conduct, the utility of which is outweighed by the gravity of consequences to Plaintiffs and members of the respective Classes. Such conduct is immoral, unethical, oppressive, unscrupulous, or substantially injurious to Plaintiffs and the members of the respective Classes.

66. Defendant's unfair or deceptive practices occurred primarily and substantially in California. Decisions concerning the retention and safeguarding of user information were made in California, LinkedIn maintains all or a substantial part of its computer systems containing user information in California, and the security breach of its computer systems took place primarily and substantially in California.

67. As a result of LinkedIn's conduct as alleged herein, Plaintiffs and the members of the respective Classes have lost money and/or property. The Data Breach Class members have lost money in the form of the value of their personal data and have lost property in the form of

their breached and compromised PII, which is of great value to LinkedIn, LinkedIn's advertisers, and malicious actors. Additionally, Premium Services Class members have lost money in the form of monthly membership fees paid partially in exchange for LinkedIn promising to use industry standard protocols and technology to protect their PII. Because LinkedIn failed to deliver on its bargained-and paid-for promise, Premium Services Class members have suffered economic damage.

68. Pursuant to Cal. Bus. & Prof. Code §§ 17203 and/or 17204, Plaintiffs seek an order permanently enjoining Defendant from continuing to engage in the unfair and unlawful conduct described herein. Plaintiffs seeks an order requiring Defendant to (1) immediately stop the unlawful practices described in this Complaint; (2) ensure that LinkedIn user data does not appear in Internet search engines; (3) ensure that LinkedIn employs commercially reasonable methods to safeguard its user data; (4) pay restitutionary disgorgement of all monies accruing to LinkedIn because of its unlawful, unfair, and deceptive practices; and (5) pay attorney's fees, and costs pursuant to Cal. Code Civ. Proc. § 1021.5.

SECOND CAUSE OF ACTION
Violation of the Consumers Legal Remedies Act
Cal. Civ. Code §§ 1750, *et seq*.
(On Behalf of Plaintiffs and both Classes)

69. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

70. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* ("CLRA") prohibits the act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, concealment, suppression or omission of any material fact with intent that others rely upon such act in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby.

71. As described herein, Defendant has engaged in deceptive practices, unlawful methods of competition, and/or unfair acts as defined by the CLRA, to the detriment of Plaintiffs and the respective Classes.

72. Defendant, acting with knowledge, intentionally and unlawfully brought harm

upon Plaintiffs and the Classes by deceptively inducing Plaintiffs and the Classes to register with LinkedIn based upon deceptive and misleading representations that it would take commercially reasonable steps to safeguard its users' sensitive PII in line with industry standards and technology. Specifically, Defendant violated the CLRA by violating § 1770(a)(5) by representing that goods or services have characteristics and benefits, which they do not have. In particular, LinkedIn represented that it used industry standard protocols and technology to protect its users' PII, which it did not actually do.

73. Plaintiffs and the Classes purchased LinkedIn's products and services by paying LinkedIn with valuable PII, thereby making them consumers under the CLRA. Further, Plaintiff Szpyrka and the Premium Service Class members paid money to Defendant in the form of monthly subscription fees for Defendant's services.

74. Plaintiffs and the Classes relied on LinkedIn's promise to use industry standard protocols and technology to safeguard their personal data in registering a LinkedIn account, and, because LinkedIn intended for Plaintiffs and the Classes to rely on such promises, LinkedIn's misstatements occurred as part of a transaction intended to result in a sale or lease of goods to consumers.

75. Plaintiffs and the Classes have suffered harm as a direct and proximate result of the Defendant's violations of law and wrongful conduct.

76. Under Cal. Civ. Code §§ 1780(a) and (b), Plaintiffs and the Classes seek injunctive relief requiring Defendant to cease and desist the illegal conduct described herein, and any other appropriate remedy for violations of the CLRA.

77. Pursuant to Cal. Civ. Code § 1782, Plaintiff Shepherd notified Defendant in writing of the particular violations of § 1770 of the CLRA and demanded Defendant rectify the actions described above by providing monetary relief, agree to be bound by its legal obligations and to give notice to all affected customers of its intent to do so. Plaintiff Shepherd sent this notice by certified mail, return receipt requested, to defendant on July 18, 2012. Defendant has

failed to adequately respond to Plaintiff Shepherd's demand within 30 days of the letter pursuant to §1782 of the CLRA. Accordingly, Plaintiffs seek compensatory and exemplary damages, costs, attorneys' fees and any other relief that the Court deems proper.

THIRD CAUSE OF ACTION
Breach of Contract
(On Behalf of Plaintiff Shepherd and the Data Breach Class)

78. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

79. In order to use its social networking applications, Defendant required that Plaintiff Shepherd and the Data Breach Class members affirmatively assent to its User Agreement and Privacy Policy (the "Agreement"). Plaintiff Shepherd and the Data Breach Class members assented to the Agreement by registering for and using LinkedIn's service.

80. The Agreement's provisions constitute a valid and enforceable contract between Plaintiff Shepherd and the Data Breach Class members on the one hand, and Defendant on the other.

81. Under the terms of the Agreement, Plaintiff Shepherd and the Data Breach Class members agreed to pay LinkedIn in the form of their valuable PII in exchange for LinkedIn's products and services and LinkedIn's promise to use industry standard protocols and technology to protect their PII.

82. Under the terms of the Agreement, in order to use Defendant's social networking applications, Plaintiff Shepherd and the Data Breach Class members transmitted several pieces of sensitive PII to Defendant, including but not limited to their e-mail addresses and corresponding passwords. In turn, under the Agreement, Defendant promised that LinkedIn would protect its users' PII with "industry standard protocols and technology."

83. Defendant materially breached the terms of the Agreement by its wrongful conduct alleged herein, including failing to properly secure its databases, thereby allowing Plaintiff Shepherd's and the Data Breach Class's sensitive PII to be compromised and disclosed, which exposed Plaintiff Shepherd and the Data Breach Class members to a heightened risk of

identity theft, and caused them distress related to their unsecured personal data, as well as distress related to the security of their other personal accounts being exposed and accessed without authorization.

84. As a result of Defendant's misconduct and breach of the Agreement described herein, Plaintiff Shepherd and the Data Breach Class members suffered injury. Plaintiff Shepherd and the Data Breach Class members did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of their own Personal Information, which has ascertainable value to be proven at trial.

FOURTH CAUSE OF ACTION
Breach of Contract
(On Behalf of Plaintiff Szpyrka and the Premium Services Class)

85. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

86. In order to use its social networking applications, Defendant required that Plaintiff Szpyrka and the Premium Services Class members affirmatively assent to its User Agreement and Privacy Policy (the "Agreement"). Plaintiff Szpyrka and the Premium Services Class members assented to the Agreement by registering for and using LinkedIn's service.

87. The Agreement's provisions constitute a valid and enforceable contract between Plaintiff Szpyrka and the Premium Services Class members on the one hand, and Defendant on the other.

88. Under the terms of the Agreement, Plaintiff Szpyrka and the Premium Services Class members agreed to pay LinkedIn a monthly fee in exchange for upgraded, premium versions of LinkedIn's products and services, and LinkedIn's promise to use "industry standard protocols and technology" to protect their PII.

89. The monthly fees, or a portion thereof, that Szpyrka and the Premium Services Class members paid to LinkedIn was used by LinkedIn to pay for the administrative costs of data management and security, and to otherwise comply with its promise to use industry standard protocols and technology to protect their PII.

90. As described herein, Defendant materially breached the terms of the Agreement by failing to use industry standard protocols and technology to protect Plaintiff Szpyrka's and the other Premium Services Class members' PII as promised.

91. As a result of Defendant's misconduct and breach of the Agreement described herein, Plaintiff Szpyrka and the Premium Services Class members suffered injury in the form of monies paid to Defendant. Plaintiff Szpyrka and the Premium Services Class members did not receive the benefit of the bargain for which they contracted, and for which they paid monthly fees.

FIFTH CAUSE OF ACTION
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiffs and both Classes)

92. Plaintiffs incorporate the foregoing allegations as if fully set forth herein, excluding paragraphs 78–91.

93. Plaintiffs hereby plead this Cause of Action in the alternative to the Third and Fourth Causes of Action.

94. In order to use Defendant's social networking site, Plaintiffs and the members of both Classes affirmatively assented to Defendant's User Agreement and Privacy Policy.

95. The Agreement's provisions constitute a valid and enforceable contract between Plaintiffs and the other members of the Classes on the one hand, and Defendant on the other.

96. Implicit in the Agreement were contract provisions that prevented Defendant from engaging in conduct that frustrated or injured Plaintiffs' and the Classes' rights to receive the benefits of the Agreement.

97. Defendant's obligation to use "industry standard protocols and technology" to safeguard and secure Plaintiffs' and the Classes' sensitive PII was a material term of the Agreement.

98. Furthermore, implicit in the terms of the Agreement was Defendant's obligation to comply with Cal. Bus. & Prof. Code §§ 17200, *et seq.* and Cal. Civ. Code §§ 1750, *et seq*.

99. Defendant breached the implied covenant of good faith and fair dealing by failing to safeguard and secure sensitive PII from unauthorized access and theft and further by failing to fully comply with the proscriptions of applicable statutory law. In so doing, LinkedIn acted consciously and deliberately.

100. Defendant's misconduct and breach of the implied covenant of good faith and fair dealing as described herein resulted in injury to Plaintiffs and the Classes. Plaintiffs and the other members of the Classes did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of their personal information that has ascertainable value to be proven at trial, and in the case of Premium Services Class members, in the form of monthly fees paid to Defendant.

SIXTH CAUSE OF ACTION
Breach of Implied Contracts
(On Behalf of Plaintiffs and both Classes)

101. Plaintiffs incorporate the foregoing allegations as if fully set forth herein, excluding paragraphs 78–91.

102. Plaintiffs hereby plead this Cause of Action in the alternative to their Third and Fourth Causes of Action.

103. In order to use Defendant's social-networking site, Plaintiffs and the other members of the Classes transmitted several pieces of sensitive PII to Defendant, including their e-mail addresses and corresponding passwords. Additionally, Plaintiffs and the Premium Services Class members paid monthly fees in order to use Defendant's upgraded services.

104. By providing that sensitive PII, and upon Defendant's acceptance of such information and monthly fees, Plaintiffs and the other members of the Classes, on the one hand, and Defendant, on the other hand, entered into implied contracts whereby Defendant was obligated to take commercially reasonable steps to secure and safeguard Plaintiffs' and the Classes' PII.

105. Without such implied contracts, Plaintiffs and the other members of the Classes

would not have provided their personal information to Defendant, or in the case of the Premium Services Class members, would not have paid monthly fees to LinkedIn.

106. By failing to properly secure Plaintiffs' and the Classes' sensitive PII, Defendant breached its implied contracts with Plaintiffs and the other members of the Classes.

107. Defendant's breaches and other misconduct described herein resulted in injury to Plaintiffs and the other members of the Classes. Plaintiffs and the other members of the Classes did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of their PII that has ascertainable value to be proven at trial, and in the case of Premium Services Class members, in the form of monthly fees paid to Defendant.

SEVENTH CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and both Classes)

108. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

109. In order to use Defendant's social networking site, Plaintiffs and the Classes transmitted sensitive PII to Defendant, including their e-mail addresses and corresponding passwords. Additionally, Premium Services Class members paid monthly fees in order to use Defendant's upgraded services.

110. By agreeing to accept Plaintiffs' and the Classes' sensitive PII, Defendant assumed a duty, which required it to exercise reasonable care to secure and safeguard that information and to utilize industry standard protocols and technology to do so.

111. Defendant failed to properly encrypt Plaintiffs' and the Classes' passwords in line with industry standards and best practices, thereby breaching its duties to Plaintiffs and the other members of the Classes.

112. By failing to take proper security measures to protect Plaintiffs' and the Classes' sensitive PII as described herein, Defendant acted with gross negligence and departed from all reasonable standards of care.

113. As a direct and proximate result of Defendant's failure to exercise reasonable care and use commercially reasonable security measures, its databases were accessed (*i.e.*, "hacked") without authorization and Plaintiffs' and the Classes' sensitive PII was compromised and their information was exposed to unauthorized access.

114. A security breach and unauthorized access was reasonably foreseeable by Defendant, particularly in light of the fact that protections necessary to secure and safeguard databases were well-known within the industry and had been successfully used to protect sensitive PII for years prior to this breach.

115. Neither Plaintiffs nor the other members of the Classes contributed to the security breach or insufficient security described herein.

116. As a direct and proximate result of Defendant's misconduct described herein, Plaintiffs and the other members of the Classes were injured because their PII was not properly secured and was thus subject to public disclosure without consent, and because they were deprived the benefit of the services for which they bargained and for which they paid valuable consideration in the form of their personal information, which has ascertainable value to be proven at trial. Additionally, Premium Services Class members lost money in the form of monthly fees paid in order to use Defendant's upgraded services with industry-standard PII.

EIGHTH CAUSE OF ACTION
Negligence *Per Se*
(On behalf of Plaintiffs and Both Classes)

117. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

118. Defendant's violations of Cal. Bus. & Prof. Code §§ 17200, *et seq.* and Cal. Civ. Code §§ 1750, *et seq.*, resulted in injury to Plaintiffs and the other members of the Classes.

119. The harm Defendant caused to Plaintiffs and the Classes are injuries that result from the type of occurrences those statutes were designed to prevent.

120. Plaintiffs and the other members of the Classes are the type of persons for whose protection those statutes were adopted.

121. The harm caused to Plaintiffs and the other members of the Classes was reasonably foreseeable as a result of LinkedIn's breach of its statutory duties, as the consequences of lax information security practices are particularly well-known within the social networking and data management industry.

122. Defendant's violations of the foregoing statutes as described herein resulted in injury to Plaintiffs and the other members of the Classes. Plaintiffs and the other members of the Classes did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of their personal information, which has ascertainable value to be proven at trial. Additionally, Premium Services Class members lost money in the form of monthly fees paid in order to use Defendant's upgraded services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Katie Szpyrka and Scott Shepherd, individually and on behalf of the Data Breach Class and Premium Services Class, pray for the following relief:

A. Certify this case as a class action on behalf of the Classes defined above, appoint Katie Szpyrka and Scott Shepherd as Class representatives, and appoint their counsel as Class counsel;

B. Declare that LinkedIn's actions, as described herein, violate the California Unfair Competition Law (Cal. Bus. & Prof. Code §§ 17200, *et seq.*) and the Consumer Legal Remedies Act (Cal. Civil Code §§ 1750 *et seq.*), and constitute breach of contract, or in the alternative, breach of the implied covenant of good faith and fair dealing, or in the alternative, breach of implied contract, as well as negligence and negligence *per se*.

C. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and the other members of the Classes, including, *inter alia*: (i) an order prohibiting LinkedIn from engaging in the wrongful and unlawful acts described herein; (ii) ensuring that LinkedIn user data does not appear in Internet search engines; and (iii) requiring LinkedIn to protect all data collected through the course of its business in accordance with

industry standards;

D. Award appropriate restitution and/or damages to Plaintiffs and the other members of the Classes in an amount to be determined at trial;

E. Award Plaintiffs and the Classes their reasonable litigation expenses and attorneys' fees;

F. Award Plaintiffs and the Classes pre- and post-judgment interest, to the extent allowable; and

G. Award such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiffs demand a trial by jury for all issues so triable.

Respectfully submitted,

Dated: September 19, 2012

Katie Szpyrka and Scott Shepherd, individually and on behalf of all others similarly situated,

/s/ Ari J. Scharg
One of Plaintiffs' Attorneys

SEAN P. REIS (SBN 184044)
(sreis@edelson.com)
EDELSON MCGUIRE LLP
30021 Tomas Street, Suite 300
Rancho Santa Margarita, California 92688
Telephone: (949) 459-2124

JAY EDELSON*
(jedelson@edelson.com)
RAFEY S. BALABANIAN
(rbalabanian@edelson.com)
ARI J. SCHARG
(ascharg@edelson.com)
CHRISTOPHER L. DORE
(cdore@edelson.com)
EDELSON MCGUIRE LLC
350 North LaSalle Street, Suite 1300
Chicago, Illinois 60654
Telephone: (312) 589-6370
*Interim Lead Counsel for Plaintiffs and the Putative Class

LAURENCE D. KING (SBN 206423)**
(lking@kaplanfox.com)
LINDA M. FONG (SBN 124232)
(lfong@kaplanfox.com)
KAPLAN FOX & KILSHEIMER LLP
350 Sansome Street, Suite 400
San Francisco, CA 94104
Tel: (415) 772-4700
**Liaison Counsel for Plaintiffs and the Putative Class

Additional Counsel for Plaintiffs and the Putative Class:

Joseph J. Siprut
(jsiprut@siprut.com)
SIPRUT PC
122 S. Michigan Ave., Suite 1850
Chicago, Illinois 60603
Tel: (312) 588-1440

David C. Parisi
(dcparisi@parisihavens.com)
PARISI & HAVENS LLP
15233 Valleyheart Drive
Sherman Oaks, CA 91403
Tel: (818) 990-1299

Dan Marovitch
(dmarovitch@marovitchlaw.com)
MAROVITCH LAW FIRM, LLC
233 S. Wacker Dr., 84th Floor
Chicago, Illinois 60606
Tel: (312) 533-1605

CERTIFICATE OF SERVICE

I, Ari J. Scharg, an attorney, certify that on September 19, 2012, I served the above and foregoing ***Consolidated Class Action Complaint*** by causing true and accurate copies of such paper to be filed and transmitted to all counsel of record via the Court's CM/ECF electronic filing system.

/s/ Ari J. Scharg